

**This Page Is Inserted by IFW Operations
and is not a part of the Official Record**

BEST AVAILABLE IMAGES

**Defective images within this document are accurate representation of
The original documents submitted by the applicant.**

Defects in the images may include (but are not limited to):

- **BLACK BORDERS**
- **TEXT CUT OFF AT TOP, BOTTOM OR SIDES**
- **FADED TEXT**
- **ILLEGIBLE TEXT**
- **SKEWED/SLANTED IMAGES**
- **COLORLED PHOTOS**
- **BLACK OR VERY BLACK AND WHITE DARK PHOTOS**
- **GRAY SCALE DOCUMENTS**

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

THIS PAGE BLANK (USPTO)

PAGE BLANK (USPTO)

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

DE 99 / 2934



REC'D 09 DEC 1999

WIPO

PCT

Bescheinigung

Die Siemens Aktiengesellschaft in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren und System zum sicheren Bezahlen von Waren oder
Diensten"

am 22. Februar 1999 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole
H 04 Q, G 07 F und G 06 F der Internationalen Patentklassifikation erhalten.

München, den 3. November 1999

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Hoiß

Aktenzeichen: 199 07 496.8



THIS PAGE BLANK (USPTO)



193 07 496.12

1

Beschreibung

Verfahren und System zum sicheren Bezahlen von Waren oder Diensten

5

Die vorliegende Erfindung betrifft ein Verfahren zum sicheren Bezahlen von Waren oder Diensten mittels einer Mobilfunkeinrichtung und einer Basistelekommunikationsstation, die mit der Mobilfunkeinrichtung über elektromagnetische Wellen kommuniziert. Ferner betrifft die Erfindung ein System zum Bezahlen von Waren oder Diensten.

Herkömmlicherweise werden beispielsweise Waren in einem Ladenlokal bar, mit einem Scheck oder elektronisch über eine Kreditkarte oder eine speziell zu diesem Zweck von einem Geldinstitut ausgegebenen Karte bezahlt. Nachteilig an derartigen Bezahlarten ist, daß der Käufer entweder Bargeld oder spezielle Karten mit sich führen muß.

20 Ferner gibt es die Möglichkeit, mittels sogenannter Telefonbanking-Verfahren Überweisungen über Telefone auszuführen. Hierzu wählt sich der Benutzer beispielsweise in die Telekommunikationseinrichtung seines Geldinstitutes ein. Daraufhin wird aus Sicherheitsgründen eine Authentifikation der Person durchgeführt, die die Überweisung tätigen will. Ergibt sich, daß der Benutzer berechtigt ist, die entsprechenden Überweisungen zu tätigen, übermittelt der Benutzer die Daten, die für die Überweisung notwendig sind. Die Daten können beispielsweise durch Sprache einer anderen dem Geldinstitut zugehörigen Person übermittelt werden. Ferner ist es möglich, daß das Telefon des Benutzers der Telekommunikationseinrichtung des Geldinstituts Kurznachrichten übersendet, die alle für die Überweisung erforderlichen Daten beinhalten. Aufgrund dieser Kurznachrichten kann das Geldinstitut dann die Überweisung ausführen.

Zur sicheren Übertragung persönlicher Informationen oder von Zugangsberechtigungsinformationen werden die entsprechenden Daten vor der Übertragung verschlüsselt. Unter Verschlüsselung, oft auch als Chiffrierung bezeichnet, versteht man die
5 Umwandlung von Daten in eine unlesbare Form. Nahezu immer benötigen sowohl die Ver- als auch die Entschlüsselung einige geheime Informationen, die gewöhnlich als Schlüssel bezeichnet werden.

- 10 Bei einem symmetrischen Verschlüsselungsverfahren wird der gleiche Schlüssel sowohl zur Chiffrierung als auch zur Dechiffrierung verwendet. Der DES (Data Encryption Standard) gehört zu den symmetrischen Verschlüsselungsverfahren. Bei diesem Verfahren besteht die Transformation des Originaltextes in den Chiffretext aus einer Aufeinanderfolge von mathematischen Operationen wie Permutationen, nichtlinearen Substitutionen und logischen Produktbildungen. Dabei wird ein
15 für den Anwender individueller Schlüssel verwendet.
- 20 Asymmetrische Verschlüsselungsverfahren bilden den Gegensatz zu den symmetrischen Verfahren. Dabei werden für Chiffrierung und Dechiffrierung unterschiedliche Schlüssel verwendet, die so beschaffen sind, daß Daten, die mit dem einen Schlüssel chiffriert wurden, nur mit dem anderen wieder dechiffriert
25 werden können.

- Telefonbanking-Verfahren können auch mit Mobilfunk-einrichtungen wie Mobiltelefonen durchgeführt werden. Mobiltelefone nach dem GSM-Standard umfassen einerseits das eigentliche Telefon mit Eingabe- und Anzeigeeinrichtungen und
30 andererseits eine sogenannte SIM-Karte, die eine Personenidentifizierungsnummer (Personal Identification Number, PIN) verschlüsselt gespeichert hat. Es ist jedoch möglich, zusätzliche Anwendungen, die hohen Sicherheitsanforderungen genügen
35 müssen, von der SIM-Karte ausführen zu lassen. (SIM Application Tool Kit, GSM 11.14). Es ist möglich, die für eine Überweisung erforderlichen Daten über die Eingabeeinrichtung des

Mobiltelefons einzugeben. Daraufhin kann eine speziell für die Überweisung erforderliche Authentifikation über die SIM-Karte des Mobiltelefons erfolgen. Den Zugriff auf diese Angebote ermöglicht eine neuartige Technik. Der Anwender benötigt hierfür ein Mobilfunktelefon mit integriertem SIM-Toolkit und einer SIM-Karte, die die neuen Mehrwertfunktionen unterstützt. Um an den virtuellen Bankschalter zu kommen, schaltet der Kunde sein Mobiltelefon ein, gibt die PIN-Nummer ein und wählt aus dem Menü sein Geldinstitut aus. Hat sich das Mobilfunktelefon in den Server der Bank eingewählt, kann der Benutzer innerhalb weniger Sekunden auf sein Bankkonto zugreifen.

Des weiteren sind sogenannte CTS (Cellular Telephony System)-Anwendungen bekannt. Derartige Systeme umfassen eine Basisstation und ein Mobiltelefon für den Hausgebrauch. Die Basisstation empfängt die Gespräche des zugehörigen Mobiltelefons intern kostenlos und leitet sie ins Festnetz weiter.

Es ist die Aufgabe der vorliegenden Erfindung, ein Verfahren und ein System zum sicheren Bezahlen von Waren oder Diensten zu schaffen, das für den Käufer und den Verkäufer einfach, sicher und kostengünstig ist.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den Merkmalen des Anspruchs 1 bzw. durch ein System mit den Merkmalen des Anspruchs 9 gelöst, wobei sich vorteilhafte Ausgestaltungen und Weiterbildungen aus den Unteransprüchen ergeben.

Im einzelnen ist das erfindungsgemäße Verfahren zum Bezahlen von Waren oder Diensten mittels einer Mobilfunkeinrichtung und einer Basistelekommunikationseinrichtung, die mit der Mobilfunkeinrichtung über elektromagnetische Wellen kommuniziert, dadurch gekennzeichnet, daß die Basistelekommunikationsstation zum Bezahlen erforderliche Daten an die Mobilfunkeinrichtung sendet, die Mobilfunkeinrichtung eine Bestäti-

gung für die Bezahlung beim Benutzer abfragt, nach der Bestätigung die Mobilfunkeinrichtung einen Bezahlvorgang durch Aussenden von Bezahlanweisungsdaten ausführt und die Mobilfunkeinrichtung oder die Telekommunikationseinrichtung eines Geldinstituts oder eines Rechnungsstellers Quittungsdaten für den Funkbezahlvorgang an die Basistelekommunikationsstation sendet.

Vorteilhaft an dem erfindungsgemäßen Verfahren ist, daß es besonders einfach ist, da die zum Bezahlen erforderlichen Daten automatisch an eine Mobilfunkeinrichtung eines Käufers gesandt werden, so daß der Verkäufer dem Käufer diese Daten nicht mitteilen muß. Des weiteren genügt das Verfahren den gleichen Sicherheitsanforderungen wie Telefonbanking-Verfahren über Mobiltelefone. Die hierbei entwickelten Sicherheitsstandards können direkt übernommen werden, was zu einer hohen Akzeptanz des erfindungsgemäßen Verfahrens beitragen wird. Da ferner die Mobilfunkeinrichtung oder die Telekommunikationseinrichtung eines Geldinstituts des Käufers Quittungsdaten für den Funkbezahlvorgang an die Basistelekommunikationsstation des Verkäufers sendet, ist die Anwesenheit eines Verkäufers in Person nicht mehr unbedingt erforderlich, weshalb das erfindungsgemäße Verfahren erhebliche Möglichkeiten zur Kostensenkung bietet und auch für Automaten geeignet ist.

Die Übertragung von Informationen oder Daten kann im Rahmen der vorliegenden Erfindung auch in Form von Kurznachrichten, Nachrichten oder mittels eines oder mehrerer Datenpakete erfolgen. Die Kommunikation der Mobilfunkeinrichtung mit der Basistelekommunikationsstation kann auch gemäß einem Mobilfunkstandard, wie dem GSM-Standard, einem Schnurlos-Standard, dem Bluetooth-Standard oder einem Infrarotstandard, wie dem IrDA-Standard erfolgen.

In einer Ausgestaltung des erfindungsgemäßen Verfahrens kann beim Ausführen des Bezahlvorgangs die Mobilfunkeinrichtung

direkt mit einer Telekommunikationseinrichtung eines Geldinstituts oder eines Rechnungsstellers beispielsweise gemäß einem Mobilfunkstandard, wie dem GSM-Standard kommunizieren.

5 Andererseits kann beim Ausführen des Bezahlvorgangs die Mobilfunkeinrichtung die Bezahlanweisungsdaten an die Basiste-
lekkommunikationsstation senden, die diese Daten dann über eine Festnetzverbindung oder gemäß einem Mobilfunkstandard, wie dem GSM-Standard, an eine Telekommunikationseinrichtung des Geldinstituts oder des Rechnungsstellers übermittelt. Ferner
10 kann die Kommunikation der Mobilfunkeinrichtung mit der Basistelekkommunikationsstation mittels Infrarotstrahlung erfolgen.

Vorteilhaft an der letzteren Möglichkeit ist, daß sie besonders kostengünstig ist, da einzig die günstigen Gebühren des
15 Festnetzes anfallen. Ferner sind jedoch auch bei der ersten Möglichkeit der direkten Kommunikation der Mobilfunkeinrichtung mit der Telekommunikationseinrichtung des Geldinstituts, die Telefongebühren in der Regel niedriger als beispielsweise
20 Kreditkartenkommissionen, so daß auch in diesem Fall das erfindungsgemäße Verfahren sowohl für den Käufer als auch für den Verkäufer besonders kostengünstig ist.

Falls die zum Bezahlen erforderlichen Daten nicht in dem Format sind, daß für den Funkbezahlvorgang notwendig ist, können
5 die von der Basistelekkommunikationsstation empfangenen Daten von der Mobilfunkeinrichtung vor dem Aussenden in ein Format umgesetzt werden, das für einen Funkbezahlvorgang geeignet ist.

30 Vorteilhafterweise erfolgt vor dem Schritt des Ausführens des Bezahlvorgangs eine Authentifikation des Benutzers der Mobilfunkeinrichtung. Diese Authentifikation kann über die Eingabe einer Personenidentifizierungsnummer oder über biometrische Merkmale erfolgen. Durch diese Maßnahme wird sichergestellt, daß
35 der Benutzer der Mobilfunkeinrichtung tatsächlich berechtigt ist, den Bezahlvorgang auszulösen. Dabei erfüllen die Verwen-

dung einer Personenidentifizierungsnummer oder die Verwendung von biometrischen Merkmalen sehr hohe Sicherheitsanforderungen.

5 Ferner kann in einer vorteilhaften Ausgestaltung des erfindungsgemäßen Verfahrens eine elektronische Kasse die zum Bezahlen erforderlichen Daten an die Basistelekommunikationsstation übermitteln. Hierdurch wird der Bezahlvorgang weiter erleichtert und automatisiert, wodurch das erfindungsgemäße Verfahren noch einfacher und kostengünstiger wird.

10

Die zum Bezahlen erforderlichen Daten können beispielsweise den zu zahlenden Geldbetrag und/oder die Kontonummer und/oder die Bankleitzahl des Empfängers und/oder des Verwendungszwecks, wie z. B. die Rechnungsnummer, umfassen.

15

Das erfindungsgemäße System zum Bezahlen von Waren oder Diensten umfaßt eine Basistelekommunikationsstation mit einer Funkeinrichtung zum Senden von zum Bezahlen erforderlichen Daten an eine Mobilfunkeinrichtung und zum Empfangen von Daten von der Mobilfunkeinrichtung, wobei die Mobilfunkeinrichtung eine Empfangseinrichtung zum Empfangen der von der Basistelekommunikationsstation ausgesandten Daten, eine mit der Empfangseinrichtung verbundene Abfrageeinrichtung zum Abfragen einer Bestätigung für die Bezahlung und eine mit der Abfrageeinrichtung verbundene Sendeeinrichtung zum Senden von Daten für einen Bezahlvorgang und zum Senden von Quittungsdaten für den Funkbezahlvorgang an die Basistelekommunikationsstation aufweist.

30 Ausführungsbeispiele der Erfindung werden nun mit Bezug auf die beigefügten Zeichnungen erläutert.

Figur 1 zeigt ein erstes Ausführungsbeispiel der vorliegenden Erfindung,

35

Figur 2 zeigt ein zweites Ausführungsbeispiel der vorliegenden Erfindung und

Figur 3 zeigt schematisch den Aufbau der Mobilfunkeinrichtung.

5 Im Folgenden werden Ausführungsbeispiele des erfindungsgemäßen Systems zum Bezahlen von Waren oder Diensten erläutert. In diesem Ausführungsbeispiel soll das erfindungsgemäße System in dem Ladenlokal eines Verkäufers installiert sein, wobei der Käufer über eine Mobilfunkeinrichtung des erfindungsgemäßen Systems Waren bezahlt.

Bei Ausführungsvarianten der Erfindung werden zum Bezahlen erforderliche Daten und/oder Bezahlungsdaten und/oder Quittungsdaten mit einem Schlüssel versehen (der Schlüssel wird beispielsweise an die entsprechenden Daten angehängt) und/oder mit einem Schlüssel verschlüsselt. Je nach Ausführungsvariante dient der Schlüssel der Verifizierung und/oder der Entschlüsselung der damit verschlüsselten Daten.

20 In dem Ladenlokal des Verkäufers ist eine Basistelekommunikationsstation 1 installiert. Vorteilhafterweise ist diese Basistelekommunikationsstation 1 mit einer elektronischen Kasse 2 verbunden, so daß die von der Kasse 2 erfaßten Daten direkt an die Basistelekommunikationsstation 1 übermittelt werden.

25 Die Basistelekommunikationsstation 1 entspricht der Basisstation des CTS mit Datenübertragungsmöglichkeit. Sie kann über elektromagnetische Wellen mit einer Mobilfunkeinrichtung 3 kommunizieren. In dem hier beschriebenen Ausführungsbeispiel wird angenommen, daß die Mobilfunkeinrichtung 3 ein Mobiltelefon nach dem GSM-Standard ist. Die Mobilfunkeinrichtung 3 könnte jedoch auch eine andere elektronische Einrichtung wie beispielsweise ein Terminplaner sein, der mit Mitteln für eine Funkübertragung von Daten ausgestattet ist. Die Verwendung eines Mobiltelefons nach dem GSM-Standard hat jedoch den Vorteil, daß an dem Gerät keine oder nur sehr wenige Modifikationen vorgenommen werden müssen.

Für den Bezahlvorgang sendet die Basistelekommunikationsstation 1 des Verkäufers die für einen Bezahlvorgang erforderlichen Daten und einen Schlüssel (key) zu einer eventuell folgenden Verschlüsselung von zu übertragenden Daten an das Mobiltelefon 3 des Käufers. Diese Daten umfassen beispielsweise die Höhe des Geldbetrags, die von der elektronischen Kasse 2 übermittelt worden ist, die Telefonnummer der Basistelekommunikationsstation, oder die Kontonummer und die Bankleitzahl des Verkäufers. Diese Daten werden von dem Mobiltelefon 3 empfangen und mittels der Anzeige 5 des Mobiltelefons 3 angezeigt. Daraufhin fragt das Mobiltelefon 3 eine Bestätigung dafür ab, daß der angezeigte Geldbetrag von dem Konto des Inhabers des Mobiltelefons 3 auf das entsprechende angezeigte Konto überwiesen werden soll. Die Bestätigung kann von dem Benutzer über die Eingabeeinheit 4 des Mobiltelefons 3 erfolgen.

Vorteilhafterweise erfolgt daraufhin die Authentifikation des Benutzers. Beispielsweise kann das Mobiltelefon 3 eine spezielle, nur für Überweisungen erforderliche Personenidentifizierungsnummer abfragen oder es können biometrische Merkmale des Benutzers erfaßt werden, wodurch der Benutzer besonders sicher und einfach identifiziert werden kann. Ergibt sich die Berechtigung des Benutzers, werden die für den Bezahlvorgang nötigen Daten oder ein Teil davon eventuell mit dem zusammen mit diesen Daten von der Basistelekommunikationsstation übermittelten Schlüssel verschlüsselt, und diese Bezahlanweisungsdaten von dem Mobiltelefon 3 an eine Telekommunikations-einrichtung 6 eines Geldinstituts oder eines Rechnungstellers gesandt, und der entsprechende Betrag abgebucht oder in Rechnung gestellt. Die Bezahlanweisungsdaten können dabei auch alle oder einen Teil der zum Bezahlen erforderlichen Daten und die Rufnummer der Mobilfunkeinrichtung enthalten. Es ist auch möglich, daß der Schlüssel nur zusammen mit den Bezahlanweisungsdaten übermittelt wird, jedoch nicht zu deren oder Verschlüsselung oder zur Verschlüsselung anderer Daten herangezogen wird.

Daraufhin sendet das Mobiltelefon 3 Quittungsdaten an die Basistelekommunikationsstation 1 des Verkäufers, so daß dieser Kenntnis von dem Bezahlen seiner Waren erlangt. Ferner könnte

5 auch die Telekommunikationseinrichtung 6 des Geldinstituts oder eines Rechnungsstellers die Quittungsdaten an die Basistelekommunikationsstation 1 übermitteln. Die mit demselben Schlüssel versehenen oder verschlüsselten Quittungsdaten werden eventuell in der Basistelekommunikationsstation 1 oder

10 einer zugeordneten Einheit entschlüsselt und nach einer erfolgreichen Entschlüsselung an die Kasse gesendet, die nach erfolgreicher Verifizierung des Schlüssels den Bon ausgibt und den Betrag als bezahlt registriert. Die Quittungsdaten können dabei auch einen Teil der zum Bezahlen erforderlichen Daten

15 enthalten oder Daten, die die Art der Ware beschreiben, oder die den Preis der Ware beschreiben, und ihr Empfang bzw. ihre Verarbeitung löst die Ausgabe der Ware oder die Erbringung des Dienstes aus.

20 Durch diese eventuelle weitere Verschlüsselung der Daten mittels eines Schlüssels, der von der Basistelekommunikationsstation an die Mobilfunkeinrichtung übermittelt wird, sind die Daten auch bei einer Übermittlung, die über das Mobilfunksystem hinaus erfolgt, beispielsweise über das Festnetz zu dem Server einer Bank oder eines Rechnungsstellers, sicher vor unberechtigttem Zugriff.

5

Figur 2 zeigt ein weiteres Ausführungsbeispiel der vorliegenden Erfindung. Das in Figur 2 gezeigte Ausführungsbeispiel unterscheidet sich von dem in Figur 1 gezeigten Ausführungsbeispiel einzig dadurch, daß beim Ausführen des Bezahlvorgangs das Mobiltelefon 3 die verschlüsselten Bezahlungsdaten nicht direkt an die Telekommunikationseinrichtung des Geldinstituts sendet, sondern diese Daten zurück an die

30 Basistelekommunikationsstation 1 sendet. Diese übermittelt dann die Daten über eine Festnetzverbindung C oder über eine

35

Mobilfunkverbindung an die Telekommunikationseinrichtung 6 des Geldinstituts oder eines Rechnungsstellers.

5 Dabei kann sich jedoch das Übertragungsverfahren, mit dem Daten an die Basistelekommunikationseinrichtung 1 gesendet werden, von demjenigen unterscheiden, mit dem die Daten in dem ersten Ausführungsbeispiel an das Geldinstitut gesendet werden.

10 Dies bedeutet, daß in diesem Fall der Verkäufer seine Basistelekommunikationsstation 1 dem Käufer für das Übermitteln einer Kurznachricht zur Verfügung stellt. Auf diese Weise wird der Bezahlvorgang besonders kostengünstig gestaltet, da dem Käufer keinerlei Kosten entstehen und der Verkäufer ein-
15 zig die relativ niedrigen Gebühren des Festnetzes für eine Kurznachricht aufbringen muß.

In diesem Fall können die Quittungsdaten für den Bezahlvorgang zusammen mit den Bezahlanweisungsdaten an die Basistele-
20 kommunikationsstation von der Mobilfunkeinrichtung gesandt werden. Ferner ist es auch möglich, daß die Bezahlanweisungsdaten als Quittungsdaten interpretiert werden, so daß keine gesonderten Quittungsdaten ausgesandt werden müssen. Des weiteren könnten die Quittungsdaten von dem Geldinstitut an die
25 Basistelekommunikationsstation 1 übermittelt werden.

Figur 3 zeigt mögliche Ausbildungen der Mobilfunkeinrichtung 3 der vorstehend erläuterten Ausführungsbeispiele. Die Mobil-
funkeinrichtung 3 weist eine Empfangseinrichtung 7 auf, die
30 die zum Bezahlen erforderlichen Daten, die von der Basistelekommunikationsstation 1 ausgesandt worden sind, empfängt. Weisen diese Daten ein Format auf, mit dem ein Bezahlvorgang direkt ausgeführt werden kann, ist eine weitere Bearbeitung der Daten nicht erforderlich. In diesem Fall, der nicht in
35 Figur 3 gezeigt ist, werden die Daten an eine Abfrageeinrichtung 9 übertragen, die über die Anzeige 5 und die Eingabeeinrichtung 4 eine Bestätigung für die Bezahlung abfragt. Gege-

benenfalls kann über diese Abfrageeinrichtung 9 auch die vorstehend erläuterte Authentifikation des Benutzers erfolgen. Liegt eine Bestätigung für die Bezahlung vor und ist durch die Authentifikation festgestellt worden, daß der Benutzer
5 berechtigt ist, die abgefragte Bezahlung vorzunehmen, werden die Daten an die Sendeeinrichtung 10 übertragen, die die Daten für den Bezahlvorgang aussendet. Vor dem Aussenden werden die Daten mittels eines digitalen Signalprozessors eventuell verschlüsselt werden.

10

Beim ersten Ausführungsbeispiel der vorliegenden Erfindung werden die Daten dann direkt an eine Telekommunikationseinrichtung 6 eines Geldinstituts oder eines Rechnungsstellers gesandt, wohingegen beim zweiten in Figur 2 gezeigten Ausführungsbeispiel die Daten zurück an die Basistelekommunikationsstation 1 gesandt werden. Ferner besteht die Möglichkeit, daß die Sendeeinrichtung 10 Quittungsdaten für den Bezahlvorgang an die Basistelekommunikationsstation 1 sendet.
15

20

Falls die von der Basistelekommunikationsstation 1 empfangenen Daten ein anderes Format aufweisen als das für den Bezahlvorgang erforderliche Format, ist in der Mobilfunkeinrichtung 3 eine Umsetzeinrichtung 8 vorgesehen, die die empfangenen Daten in ein Format umsetzt, das für einen Bezahlvorgang geeignet ist. Diese Umsetzeinrichtung kann beispielsweise, wie in Figur 3 gezeigt, zwischen der Empfangseinrichtung 7 und der Abfrageeinrichtung 9 vorgesehen sein. Es besteht jedoch auch die Möglichkeit die Umsetzeinrichtung 8 zwischen der Abfrageeinrichtung 9 und der Sendeeinrichtung 10
25
30 vorzusehen.

30

Bezüglich des ersten Ausführungsbeispiels, bei dem die Mobilfunkeinrichtung 3 sowohl mit der Basistelekommunikationsstation 1 als auch mit der Telekommunikationseinrichtung 6 eines Geldinstituts oder eines Rechnungsstellers kommuniziert, kann
35 die Mobilfunkeinrichtung 3 auch getrennte Sende- und Empfangseinrichtungen 7, 10 für die Kommunikation mit der Basi-

stelekkommunikationseinrichtung 1 und der Telekommunikations-
einrichtung 6 des Geldinstituts aufweisen. Dadurch könnte
beispielsweise die Kommunikation mit der Basiskommunikations-
einrichtung 1 über Infrarotstrahlung erfolgen und die Kommu-
5 nikation mit der Telekommunikationseinrichtung 6 des Geldin-
stituts gemäß dem GSM-Standard erfolgen.

In einer weiteren Anwendung der vorliegenden Erfindung wird
diese zum Abheben von Geld an einem Geldautomaten verwendet.
10 In diesem Fall ist die Basistelekkommunikationseinrichtung 1
der Geldautomat eines Geldinstituts, der über eine Festnetz-
leitung mit dem Zentralrechner des Geldinstituts verbunden
ist. Zum Geldabheben gibt eine Person eine entsprechende An-
frage bei dem Geldautomat ein. Diese Daten sendet der Geldau-
15 tomat zusammen mit einem Schlüssel an die Mobilfunkeinrich-
tung 3, die eine Bestätigung für den Abhebevorgang bei der
Person abfragt. Vorteilhafterweise erfolgt nun die Authentifi-
kation der Person mittels der Mobilfunkeinrichtung 3. Ist
die Person als berechtigt identifiziert worden und hat sie
20 eine Bestätigung für den Abhebevorgang in die Mobilfunkein-
richtung eingegeben, sendet die Mobilfunkeinrichtung mit dem
Schlüssel versehene oder verschlüsselte Daten an den Geldau-
tomaten, so daß diesem mitgeteilt wird, daß das Geld ausge-
zahlt werden kann. Für die Abbuchung des Geldbetrags kommuni-
25 ziert der Geldautomat mit dem Zentralrechner des Geldinsti-
tuts über eine Festnetzverbindung.

In einer besonders einfachen Ausführung der Erfindung besteht
die Basistelekkommunikationsstation aus einer Infrarot-
30 Schnittstelle nach dem IrDA-Standard und einem GSM-Modul. Die
Infrarot-Schnittstelle und das GSM-Modul sind angeschlossen
an das üblicherweise in einem Automaten oder einer Regi-
strierkasse vorhandene Steuerungssystem. Die Daten können da-
bei auch über eine auf einer Infrarot-Schnittstelle basieren-
35 den AT-Zellular-Schnittstelle übertragen werden.

Über Infrarotstrahlen wird nun eine Kurznachricht an das Mobiltelefon gesandt, die im Klartext die Frage enthält, ob der Kunde die gewünschte Ware zum gewünschten Preis bezahlen will und ggf. eine Schlüsselzahl. Die Kurznachricht enthält zum

5 bezahlen erforderliche Daten, optional einen Schlüssel und die Telefonnummer eines "Absenders". Da die Kurznachricht von einem Steuerungssystem künstlich generiert wird, kann diese Telefonnummer im Automaten oder in der Registrierkasse fest einprogrammiert werden und entspricht dann der Telefonnummer

10 des Rechnungsstellers. Der Kunde liest die Kurznachricht und generiert, wenn er einverstanden ist, eine Antwort "JA". Dies ist bei vielen Mobiltelefonen mit wenigen Tastendrücken möglich oder kann durch SIM Application Toolkit vereinfacht werden. Die vom Kunden generierte Kurznachricht wird dann an die

15 "Absender"-Telefonnummer, also an den Rechnungssteller geschickt. Der Servicerechner des Rechnungssteller setzt den Betrag auf die Rechnung des Kunden, der sich wiederum durch seine in seiner Kurznachricht enthaltene Telefonnummer identifiziert. Anschließend sendet der Servicerechner des Rechnungssteller

20 eine Nachricht zur Ausgabe der gewünschten Ware an den Automaten oder die Registrierkasse. Diese Nachricht kann über GSM oder auch über ein wie auch immer geartetes Festnetz oder ein beliebiges Netz basierend auf elektromagnetischen Wellen gesendet werden. Der (optional) gesendete

5 Schlüssel wird in der Registrierkasse oder dem Automaten, wo er ja auch generiert wurde, geprüft und die gewünschte Ware wird ausgegeben.

Die Überprüfung oder Verifizierung des Schlüssels erfolgt

30 durch einen Vergleich des übermittelten Schlüssels mit einem nach der Generierung des Schlüssels in der Basistelekommunikationsstation oder einer zugeordneten Einheit gespeicherten Schlüssel. Nach einem erfolgreichen Vergleich, also bei Übereinstimmung der beiden Schlüssel wird die bezahlte Ware aus-

35 gegeben oder der bezahlte Dienst erbracht.

Im folgenden wird ein weiteres konkretes Ausführungsbeispiel der Erfindung erläutert:

- 5 - Ein Kunde steht vor einem Automaten und drückt eine Taste für eine gewünschte Ware oder der Kunde steht an einer Registrierkasse.
- 10 - Die Registrierkasse oder der Automat schicken mittels Infrarotstrahlen (beispielsweise IrDA), gemäß dem Bluetoothstandard, einem Schnurlosstandard oder einem Mobilfunkstandard eine Nachricht, Kurznachricht (Short Message) oder entsprechende Datenpakete an das Mobiltelefon des Kunden. Diese Nachricht enthält neben allen zum Bezahlen erforderlichen Daten einen Schlüssel (Key), der auf einem oder mehreren folgenden Signalpfaden zur Verschlüsselung der entsprechenden Daten verwendet werden kann. Außerdem enthält die Nachricht 15 die Rufnummer des Rechnungsstellers (Billing Center). Dies kann auch eine Bank, ein Netzbetreiber oder eine Kaufhauskette sein.
- 20 - Die Nachricht löst eine SIM Application Toolkit Anwendung auf dem Mobilfunktelefon aus, die einen Dialog mit dem Kunden einleitet. Der Kunde wird gefragt: "Wollen Sie eine Cola an diesem Automaten für Euro 1,50 kaufen?" oder "Wollen Sie bei Hertie in der Lebensmittelabteilung DM 123,45 bezahlen?".
- 25 - Mit dem Softkey "ja" oder einer spezifizierten Zifferntaste wird - ggf. nach Abfrage einer PIN - eine Nachricht generiert, die den Preis, die Warenart, die Tel.-Nr. des Automaten oder der Registrierkasse und ggf. die des Kunden enthält. Diese Daten werden mit dem Schlüssel verschlüsselt und an das Billing Center versandt. Die Abfrage einer PIN ,z. B. ab einem bestimmten Betrag, kann vom Kunden aktiviert werden. 30
- 35 - Im Billing Center wird der Betrag auf die Rechnung des Kunden gesetzt, und eine mit demselben Schlüssel verschlüsselte Nachricht an den Automaten gesendet, der nach einer erfolgreichen Entschlüsselung die gewünschte Ware ausgibt, bzw. an die Kasse gesendet, die den Bon ausgibt und den Betrag als bezahlt registriert.

Dabei ist das Billing Center (der Rechnungssteller) nicht auf ein Geldinstitut eingeschränkt. Es kann sich dabei auch um den Netzbetreiber, den Betreiber der Automaten oder der Registrierkassen, oder ein Kreditkartenunternehmen handeln.

- 5 Die Weiterleitung der Quittungsdaten für den Bezahlvorgang muß nicht über ein Mobilfunksystem, wie das GSM-System erfolgen. Das Billing-Center kann z. B. in einem großen Kaufhaus stehen, das mit den Registrierkassen vernetzt ist.

- 10 Als Schlüssel kann eine zufällig generierte Zahl mit der Bezahlanweisung an den Rechnungssteller und von dort an den Automaten zurückgeschickt werden. Da der Automat den Schlüssel generiert hat, kann er ihn selbst abprüfen. Dabei kann außerdem eine dem Automaten und dem Rechnungssteller bekannte Ver-
- 15 schlüsselung der gesamten Nachricht angewandt werden, um zusätzliche Sicherheit zu generieren. In diesem Fall muß keine Verschlüsselung im Mobiltelefon stattfinden.

- Eine Ausführungsvariante der Erfindung sieht vor, daß der
- 20 Schlüssel von der Kasse/dem Automaten oder der Basistelekomunikationsstation als Zufallszahl generiert wird, da die Kontrolle des Schlüssels wieder an der Kasse/dem Automaten erfolgt. Der Schlüssel kann im Billing Center zusätzlich nach einem in der Kasse/dem Automaten oder der Basistelekommunikationsstation bekannten Algorithmus verändert werden. Wenn
- 5 über die Verbindung der Kassen mit dem Billing Center zusätzlich der Algorithmus regelmäßig verändert wird, ist ein Mißbrauch des Bezahlvorganges ausgeschlossen.

Patentansprüche

1. Verfahren zum sicheren Bezahlen von Waren oder Diensten mittels einer Mobilfunkeinrichtung (3) und einer Basistelekommunikationsstation (1), die mit der Mobilfunkeinrichtung (3) über elektromagnetische Wellen kommuniziert, dadurch gekennzeichnet, daß
- die Basistelekommunikationsstation (1) zum Bezahlen erforderliche Daten an die Mobilfunkeinrichtung (3) sendet,
 - die Mobilfunkeinrichtung (3) eine Bestätigung für die Bezahlung beim Benutzer abfragt,
 - nach der Bestätigung die Mobilfunkeinrichtung (3) einen Bezahlvorgang durch Aussenden von Bezahlungsdaten auslöst, und
 - die Mobilfunkeinrichtung (3) oder eine Telekommunikationseinrichtung (6) eines Geldinstituts oder eines Rechnungsstellers Quittungsdaten für den Bezahlvorgang an die Basistelekommunikationsstation (1) sendet.
2. Verfahren gemäß Anspruch 1, dadurch gekennzeichnet, daß die Basistelekommunikationsstation (1) auch einen in der Basistelekommunikationsstation (1) oder einer zugeordneten Einheit generierten Schlüssel an die Mobilfunkeinrichtung (3) sendet, die Mobilfunkeinrichtung (3) diesen Schlüssel an die Telekommunikationseinrichtung (6) eines Geldinstituts oder eines Rechnungsstellers sendet, und der Schlüssel von einer Telekommunikationseinrichtung (6) eines Geldinstituts oder eines Rechnungsstellers an die Basistelekommunikationsstation (1) gesendet wird.
3. Verfahren gemäß einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß der Schlüssel zumindest auf bestimmten Übertragungswegen zur Verschlüsselung zu Übertragender Daten verwendet wird.

4. Verfahren gemäß einem der vorstehenden Ansprüche ,
d a d u r c h g e k e n n z e i c h n e t ,
daß zum Bezahlen erforderliche Daten von der Basistelekommu-
5 nikationsstation (1) derart an die Mobilfunkeinrichtung (3)
übermittelt werden, daß zumindest Teile dieser Daten als zu
lesende Kurznachricht in den Kurznachrichtenspeicher der Mo-
bilfunkeinrichtung (3) geschrieben werden, wobei als Absen-
derrufnummer die Rufnummer einer Telekommunikations-
10 einrichtung (6) eines Geldinstituts oder eines Rechnungsstel-
lers eingetragen wird.

5. Verfahren gemäß einem der vorstehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t ,
15 daß nach dem Lesen der Kurznachricht und einer entsprechenden
Bestätigung durch den Benutzer automatisch eine zum Bezahlen
erforderliche Daten enthaltende Kurznachricht an eine Tele-
kommunikationseinrichtung (6) eines Geldinstituts oder eines
Rechnungsstellers übermittelt wird.

20 6. Verfahren gemäß einem der vorstehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t ,
daß die Kommunikation zwischen der Basistelekommunikations-
station (1) und der Mobilfunkeinrichtung (3) auf der Basis
5 eines IrDA-Standards erfolgt.

7. Verfahren gemäß einem der vorstehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t ,
daß die Kommunikation zwischen der Mobilfunkeinrichtung (3)
30 und der Telekommunikationseinrichtung (6) eines Geldinstituts
oder eines Rechnungsstellers auf der Basis eines Mobilfunk-
standards erfolgt.

8. Verfahren gemäß einem der vorstehenden Ansprüche ,
35 d a d u r c h g e k e n n z e i c h n e t ,
daß nach einem erfolgreichen Vergleich des übertragenen
Schlüssels mit einem in der Basistelekommunikationsstation

(1) oder einer zugeordneten Einheit gespeicherten Schlüssel in der Basistelekommunikationsstation (1) oder einer zugeordneten Einheit die Ausgabe der Ware oder die Erbringung des Dienstes erfolgt.

5

9. Verfahren gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß der Schlüssel zusammen mit für den Bezahlvorgang erforderlichen Daten und/oder mit Quittungsdaten für den Bezahlvorgang übertragen wird.

10

10. Verfahren gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß eine elektronische Kasse (2) die zum Bezahlen erforderlichen Daten an die Basistelekommunikationsstation (1) übermittelt.

15

11. Verfahren gemäß einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß zum Bezahlen erforderliche Daten den zu zahlenden Geldbetrag und/oder eine Bezeichnung der zu bezahlenden Ware oder des zu bezahlenden Dienstes und/oder die Kontonummer und/oder die Bankleitzahl des Empfängers und/oder den Verwendungszweck und/oder eine Kundennummer und/oder die Rufnummer einer Telekommunikationseinrichtung (6) eines Geldinstituts oder eines Rechnungsstellers umfaßt/umfassen.

25

12. System zum sicheren Bezahlen von Waren oder Diensten, umfassend:

30

- eine Basistelekommunikationsstation (1) mit einer Funkeinrichtung zum Senden von zum Bezahlen erforderlichen Daten an eine Mobilfunkeinrichtung (3) und zum Empfangen von Daten von der Mobilfunkeinrichtung (3),

wobei die Mobilfunkeinrichtung (3) aufweist:

35

- eine Empfangseinrichtung (7) zum Empfangen der von der Basistelekommunikationsstation (1) ausgesandten Daten,

- eine mit der Empfangseinrichtung (7) verbundene Abfrageeinrichtung (9) zum Abfragen einer Bestätigung für die Bezahlung und

- 5 - eine mit der Abfrageeinrichtung (9) verbundene Sendeeinrichtung (10) zum Senden von Daten zum Auslösen eines Bezahlvorgangs und/oder zum Senden von Quittungsdaten für den Bezahlvorgang an die Basistelekommunikationsstation (1).

- 10 13. System gemäß Anspruch 12,
d a d u r c h g e k e n n z e i c h n e t ,
mit einer der Basistelekommunikationsstation (1) zugeordneten Recheneinrichtung zur Erzeugung und/oder Verifizierung eines Schlüssels.

- 15 14. System gemäß Anspruch 12 oder 13,
d a d u r c h g e k e n n z e i c h n e t ,
daß die Mobilfunkeinrichtung eine Umsetzeinheit aufweist, die von der Basistelekommunikationsstation (1) übermittelte zum Bezahlen erforderlich Daten derart in eine zu lesende Kurznachricht umsetzt, daß als Absenderrufnummer die mit den zum
20 Bezahlen erforderlich Daten übermittelte Rufnummer einer Telekommunikationseinrichtung (6) eines Geldinstituts oder eines Rechnungsstellers eingetragen wird.

- 25 15. System gemäß einem der Ansprüche 12 bis 14 ,
d a d u r c h g e k e n n z e i c h n e t ,
daß die Basistelekommunikationsstation (1) mit einer elektronischen Kasse verbunden ist, die zum Übermitteln der zum Bezahlen erforderlichen Daten an die Basistelekommunikationsstation (1) ausgebildet ist.
30

16. System gemäß einem der Ansprüche 12 bis 15 ,
d a d u r c h g e k e n n z e i c h n e t ,
daß zum Bezahlen erforderliche Daten den zu zahlenden Geldbetrag und/oder eine Bezeichnung der zu bezahlenden Ware oder
35 des zu bezahlenden Dienstes und/oder die Kontonummer und/oder die Bankleitzahl des Empfängers und/oder den Verwendungszweck

und/oder eine Kundennummer und/oder die Rufnummer einer Telekommunikationseinrichtung (6) eines Geldinstituts oder eines Rechnungsstellers umfaßt/umfassen.

Zusammenfassung

Verfahren und System zum sicheren Bezahlen von Waren oder
Diensten

5

10

15

20

Die vorliegende Erfindung betrifft ein Verfahren und ein System zum Bezahlen von Waren oder Diensten. Sie umfaßt eine Mobilfunkeinrichtung (3) und eine Basistelekommunikationsstation (1), die mit der Mobilfunkeinrichtung (3) über elektromagnetische Wellen kommuniziert. Die Basistelekommunikationsstation (1) sendet die zum Bezahlen erforderlichen Daten an die Mobilfunkeinrichtung (3). Diese fragt beim Benutzer eine Bestätigung für die Bezahlung ab. Nach der Bestätigung führt die Mobilfunkeinrichtung (3) einen Bezahlvorgang durch Aussenden von Bezahlungsdaten aus. Ferner sendet entweder die Mobilfunkeinrichtung (3) oder eine Telekommunikationseinrichtung (6) eines Geldinstituts Quittungsdaten für den Bezahlvorgang an die Basistelekommunikationsstation (1).

(Figur 1)

FIG 1

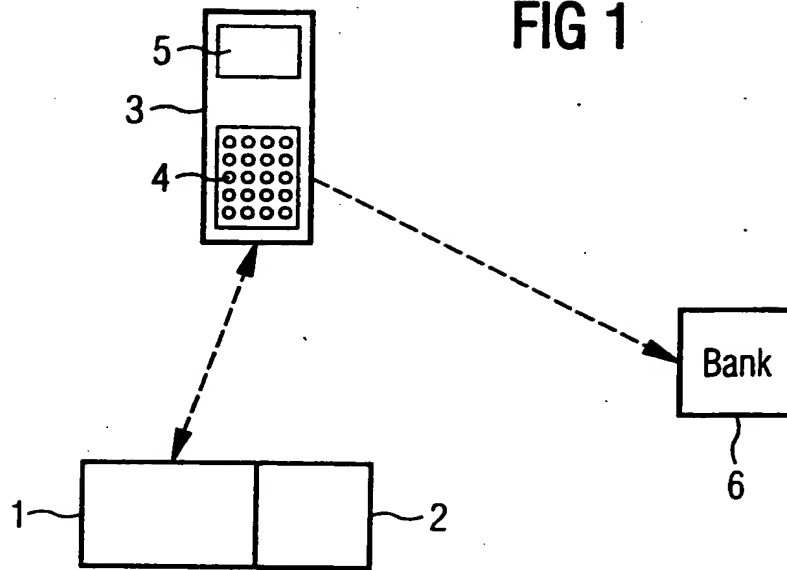


FIG 2

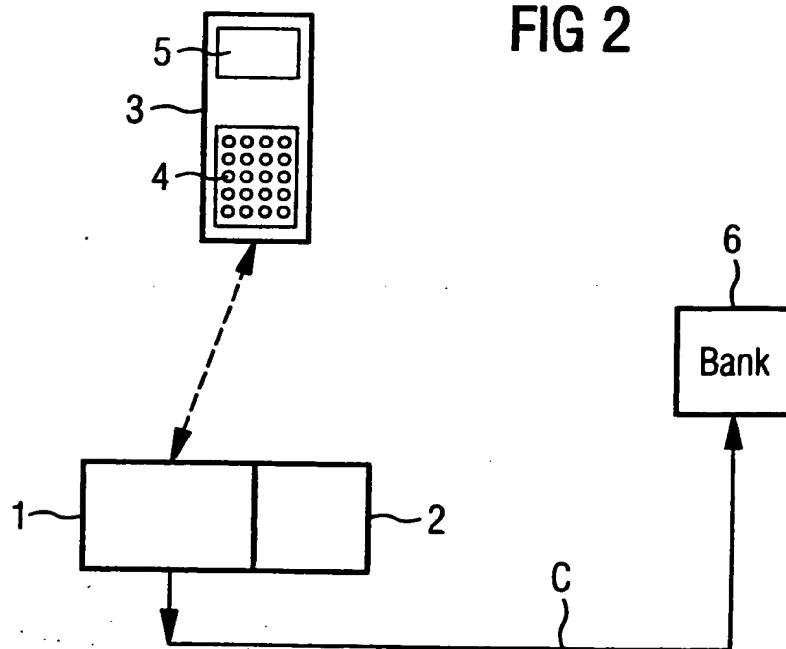
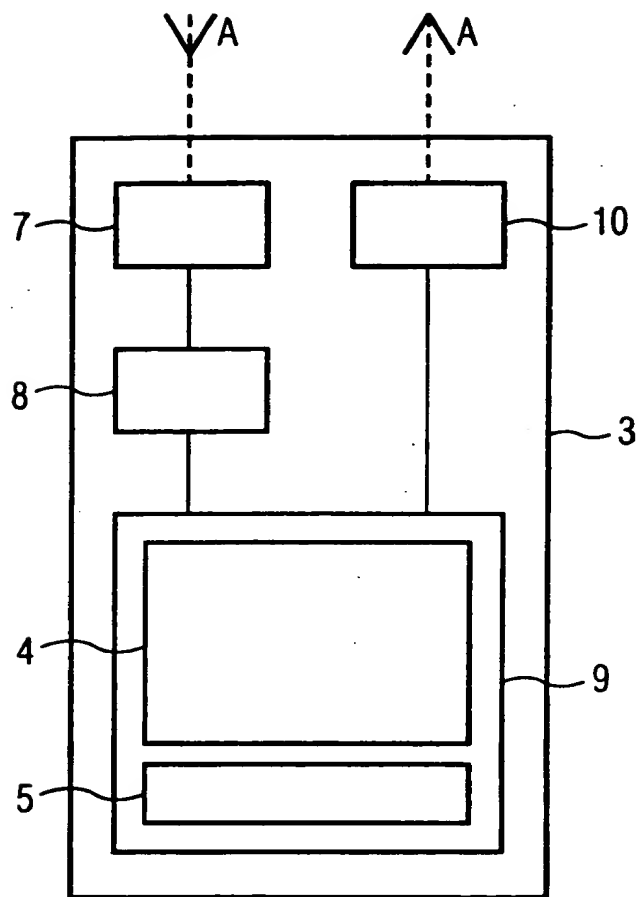


FIG 3



THIS PAGE BLANK (USPTO)